CLAIMS

What is claimed is:

1. A system for controlling access of a client to a network resource, the system comprising:

a network resource that is communicatively coupled to a network;

an authentication server that is communicatively coupled to the network and to the network firewall routing device and comprising user profile information;

a network firewall routing device that is communicatively coupled to the network and that is logically interposed between the client and the network resource;

means for creating and storing client authorization information at the network firewall routing device, based in part on the user profile information, wherein the client authorization information comprises information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client has with respect to the network resource;

means for receiving a request from the client to communicate with the network resource;

means for determining whether the client is authorized to communicate with the network resource based on the authorization information; and

means for reconfiguring the network firewall routing device to permit the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on the authorization information.

2. A system as recited in Claim 1, wherein the client authorization information comprises means in the network firewall routing device for caching client authorization information for each client that communicates with the network firewall routing device.

3. A system as recited in Claim 1, wherein the client authorization information comprises an authentication cache in the network firewall routing device for each client that communicates with the network firewall routing device.

4. A system as recited in Claim 1, wherein the client authorization information comprises a plurality of authentication caches, each authentication cache uniquely associated with one of a plurality of clients that communicate with the network routing device, each authentication cache comprising information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client is authorized to have with respect to the network resource.

5. A system as recited in Claim 1, wherein the means for determining whether the client is authorized to communicate with the network resource comprises means for matching information in the request identifying the client to information in means for filtering in the network routing device and to the authorization information stored in the network firewall routing device.

6. A system as recited in Claim 1, wherein the means for determining whether the client is authorized to communicate with the network resource comprises:

means for matching a source IP address of the client in a data packet of the request to information in a filtering mechanism of the network routing device; and

means for matching the source IP address to the authorization information stored in the network firewall routing device if the source IP address matches the information in the filtering mechanism of the network routing device.

7. A system as recited in Claim 1, wherein the means for determining whether the client is authorized to communicate with the network resource comprises:

means for matching a source IP address of the client in a data packet of the request to information in a means for filtering in the network routing device;

means for matching the source IP address to the authorization information stored in the network firewall routing device if the source IP address matches the information in the filtering mechanism of the network routing device; and

means for matching user identifying information received from the client to a profile associated with the user that is stored in the authentication server if the source IP address fails to match the authorization information stored in the network firewall routing device.

8. A system as recited in Claim 1, wherein the means for determining whether the client is authorized to communicate with the network resource comprises:

means for matching a source IP address of the client in a data packet of the request to information in a filtering mechanism of the network routing device;

means for matching the source IP address to the authorization information stored in the network firewall routing device if the source IP address matches the information in the filtering mechanism of the network routing device; and

means for matching user identifying information received from the client to a profile associated with the user that is stored in a database server and is retrieved from the database server by the authentication server, if the source IP address fails to match the authorization information stored in the network firewall routing device.

9. A system as recited in Claim 1, wherein the means for determining whether the client is authorized to communicate with the network resource comprises:

means for matching client identifying information in the request to information in a filtering mechanism of the network routing device;

means for matching the client identifying information to the authorization information stored in the network firewall routing device, if a match is found using the filtering mechanism; and

means used, only when the client identifying information fails to match the authorization information stored in the network firewall routing device, for:

creating and storing new authorization information in the network firewall routing device that is uniquely associated with the client;

requesting login information from the client;

authenticating the login information by communicating with the authentication server; and

updating the new authorization information based on information received from the authentication server.

10. A system as recited in Claim 9, wherein the means for requesting login information from the client comprises means for sending a Hypertext Markup language login form from the network firewall routing device to the client to solicit a username and a user password; and wherein the means for authenticating the login information comprises means for determining, from a profile associated with a user of the client stored in the authentication server, whether the username and password are valid.

11. A system as recited in Claim 9, wherein the means for requesting login information from the client comprises means for sending a Hypertext Markup language login form from the network firewall routing device to the client to solicit a username and a user password; and wherein the means for authenticating the login information comprises:

means for retrieving a profile associated with a user of the client from a database server; and

means for determining, from the profile associated with the user, whether the username and password are valid.

12. A system as recited in Claim 9, the system further comprising:

means for creating and storing an inactivity timer for each authentication cache, wherein the inactivity timer expires when no communications are directed from the client to the network resource through the network firewall routing device during a pre-determined period of time;

means for removing the updated authentication information when the inactivity timer expires.

13. A system as recited in Claim 1, wherein the means for determining whether the client is authorized to communicate with the network resource comprises:

means for matching a source IP address in the request to information in a filtering mechanism of the network routing device;

means for matching the source IP address to the authorization information stored in the network firewall routing device using an authentication cache in the network firewall routing device; and

means used, only when the source IP address fails to match the authorization information stored in the network firewall routing device, for:

creating and storing a new entry in the authentication cache that is uniquely associated with the client;

requesting login information from the client;

authenticating the login information by communicating with the authentication server; and

updating the new entry in the authentication cache based on information received from the authentication server.

14. A system as recited in Claim 1, wherein the means for reconfiguring the network firewall routing device comprises means for creating and storing one or more commands to the network firewall routing device which, when executed by the network firewall routing device, result in modifying one or more routing interfaces of the network firewall routing device to permit communications between the client and the network resource.

15. A system for controlling access to a network resource, the system comprising:

a network resource that is communicatively coupled to a network;

an authentication server that is communicatively coupled to the network and to the network firewall routing device and comprising user profile information;

a client capable of sending a request to communicate with the network resource;

a network firewall routing device that is logically interposed between the client and the network resource and is capable of permitting the client to communicate with the network resource;

means for creating and storing client authorization information at the network firewall routing device, wherein the client authorization information comprises information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client has with respect to the network resource;

means for determining, at the network firewall routing device, whether the client is authorized to communicate with the network resource based on the authorization information; and

means for reconfiguring the network firewall routing device to permit the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on the authorization information.

16. A system as recited in Claim 15, wherein the client authorization information comprises a plurality of authentication caches, each authentication cache uniquely associated with one of a plurality of clients that communicate with the network routing device, each authentication cache comprising information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client is authorized to have with respect to the network resource.

17. A system as recited in Claim 15, wherein the means for determining whether the client is authorized to communicate with the network resource comprises:

means for matching client identifying information in the request to information in a filtering mechanism of the network routing device; and

means for matching the client identifying information in the request to the authorization information stored in the network firewall routing device if the client identifying information in the request matches the information in the filtering mechanism of the network routing device.

18. A system as recited in Claim 15, wherein the means for determining whether the client is authorized to communicate with the network resource comprises:

means for matching client identifying information in the request to information in a filtering mechanism of the network routing device;

means for matching the source IP address to the authorization information stored in the network firewall routing device if the client identifying information in the request matches the information in the filtering mechanism of the network routing device; and

means for matching user identifying information received from the client to a profile associated with the user that is stored in a database server and is retrieved from the database server by an authentication server that is coupled to the network firewall routing device, if the client identifying information in the request fails to match the authorization information stored in the network firewall routing device.

19. A system as recited in Claim 15, wherein the means for determining whether the client is authorized to communicate with the network resource comprises:

means for matching client identifying information in the request to information in a filtering mechanism of the network routing device;

means for matching the client identifying information in the request to the authorization information stored in the network firewall routing device using an authentication cache in the network firewall routing device; and

means, used only when the client identifying information in the request fails to match the authorization information stored in the network firewall routing device, for:

creating and storing a new entry in the authentication cache that is uniquely associated with the client;

requesting login information from the client;

authenticating the login information by communicating with the authentication server; and

updating the new entry in the authentication cache based on information received from the authentication server.

20. A system as recited in Claim 19, wherein the means for requesting login information from the client comprises means for sending a Hypertext Markup language login form from the network firewall routing device to the client to solicit a username and a user password; and wherein the means for authenticating the login information by communicating with the authentication server comprises:

means for retrieving a profile associated with a user of the client from a database server; and

means for determining, from the profile associated with the user, whether the username and password are valid.

21. A system as recited in Claim 15, wherein the client is a computer system executing a Web browser.

22. A system for authentication comprising:

a network resource connected to a network;

a client capable of sending a request to communicate with the network resource;

a network firewall routing device that is logically interposed between the client and the network resource and that permits the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on client authorization information stored in the network firewall routing device, wherein the client authorization information comprises information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client has with respect to the network resource;

a database server that stores a plurality of user profiles, each user profile uniquely associated with one of a plurality of users that can use the client to send requests to communicate with the network resource;

an authentication server that is logically interposed between the network firewall routing device and the database server, and that is capable of communicating with the database server and retrieving from the database server a user profile.

23. A system as recited in Claim 22, wherein the network resource comprises a target server capable of servicing a request sent under at least one of HyperText Transfer Protocol; File Transfer Protocol; and Internet Control Message Protocol.

24. A system as recited in Claim 22, wherein the client comprises a computer system executing a Web browser.

25. A system as recited in Claim 22, wherein the network firewall routing device comprises:

one or more processors; and

a storage medium carrying one or more sequences of one or more instructions including instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

creating and storing the client authorization information at the network firewall routing device;

receiving the request from the client to communicate with the network resource;

determining whether the client is authorized to communicate with the network resource based on the client authorization information; and

permitting the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on the client authorization information.

26. A system as recited in Claim 25, wherein permitting the client to communicate with the network resource comprises the steps of creating and storing one or more commands which, when executed by the network firewall routing device, result in modifying one or more routing interfaces of the network firewall routing device to permit communications between the client and the network resource.

27. A system as recited in Claim 25, wherein determining whether the client is authorized to communicate with the network resource comprises the steps of:

determining whether client identifying information in the request matches information in a filtering mechanism of the network firewall routing device;

if a match is found using the filtering mechanism, determining whether the client identifying information matches the client authorization information stored in the network firewall routing device; and

only when the client identifying information fails to match the client authorization information stored in the network firewall routing device, then:

creating and storing new client authorization information in the network firewall routing device that is uniquely associated with the client;

requesting login information from the client;

authenticating the login information by communicating with the authentication server; and

updating the new client authorization information based on information received from the authentication server.

28. A system as recited in Claim 27, wherein:

requesting login information from the client comprises sending a Hypertext Markup Language login form to the client to solicit a username and a password; and

authenticating the login information by communicating with the authentication server comprises determining, from a profile that is associated with a user of the client and that is retrieved from the database server, whether the username and password are valid.

29. A system as recited in Claim 22, wherein the authentication server comprises:

one or more processors; and

a storage medium carrying one or more sequences of one or more instructions including instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

receiving client identifying information from the network firewall routing device, wherein the client identifying information comprises a username and a password associated with a user of the client;

retrieving a profile associated with the user from the database server;

determining whether the username and the password in the client identifying information match the username and the password stored in the profile associated with the user; and

only if a match is found, returning to the network firewall routing device information indicating that the username and the password are valid.

30. A system as recited in Claim 22, wherein the database server comprises:

one or more processors; and

a storage medium carrying one or more sequences of one or more instructions including instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

storing a profile associated with a user of the client, wherein the profile comprises a username and a password; and

retrieving the profile associated with a user of the client upon a request from the authentication server.